UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/765,621	01/27/2004	Scott Alan Leerssen	10980679-2	1355

7590 04/20/2005

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P. O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
GURSHMAN, GRIGORY	
ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 04/20/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/765,621	LEERSSEN ET AL.	
	Examiner	Art Unit	
	Grigory Gurshman	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 January 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 January 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *4/23/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 112

1. The recitation "inconsistent sensitivity labels" and "arbitrary incomparable" in claim 1 are relative terms, which renders the claim indefinite. The terms "inconsistent sensitivity labels" and "arbitrary incomparable" are not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. Applicant needs to define ~~weather~~ how the sensitivity labels, recited in claim 1, are comparable or not and ~~weather~~ how the labels are consistent or inconsistent with some criteria.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claim 1 - 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Edwards (U.S. Patent No. 6.490.626 B1) in view of Shurts (U.S. Patent No. 5.572.673).

4. Referring to the instant claims, Edwards discloses a browser system (see title and Fig. 2). The operation of the Web browser (210) is prevented from accessing or damaging other compartments of the CMW machine (200) as a result of mandatory access control (MAC), which is configured appropriately (see abstract). Edwards teaches that the MAC policy uses labels that reflect information sensitivity, and

maintains those labels for every process and file system object to prevent users not cleared for certain levels of classified information from accessing it (see column 3, lines 60-64). Edwards also teaches that the sensitivity labels are associated with every process and file system object, and are used as the primary basis for all MAC policy decisions. A sensitivity label represents the sensitivity of a process or a file system object and also the data each contains. If an application and the file it attempts to access have compatible sensitivity labels, the application can read, write, or possibly execute the file, and each new process typically inherits the sensitivity label of its parent (see column 5, lines 3-9). Sensitivity labels are prioritized for MAC in a way that determines how processes or objects having one sensitivity label can interact with processes or objects having different sensitivity labels. The prioritization is defined internally of the operating system. The diagram in FIG. 3 represents the relationship between the parts of the system illustrated in FIG. 2.

5. Referring to the independent claims 1 and 12, the limitation "enforcing sensitivity labels such that the operating system restricts the transfer of data transfer between subjects and objects associated with inconsistent sensitivity labels" is met by teaching of Edwards that if the application (i.e. subject) and the file (i.e. object) it attempts to access have compatible sensitivity labels, application can read, write, or possibly execute the file (see column 5, lines 3-9). The limitation "designating the sensitivity labels such that each sensitivity label either dominates, is dominated by, or incomparable..." is met by Fig. 3 depicting the sensitivity labels are prioritized in such a way that it determines how objects having one sensitivity label can interact with the

objects having different type of sensitivity label. The limitation "...defining the arbitrary relationships between the subjects and objects of different sensitivity labels" is met by the sensitivity labels, which are prioritized in such a way that it determines how objects having one sensitivity label can interact with the objects having different sensitivity label (see Fig. 3). Edwards, however does not explicitly teach providing discrete access between arbitrary, incomparable sensitivity labels. Referring to the instant claims, Shurts discloses a secure multi-level system for executing stored procedures (see abstract). Shurts teaches that before any object is accessed in a MAC system, the subject's sensitivity label is compared with the object's sensitivity label to determine whether the subject is allowed to access the object in the manner requested (see column 1, lines 60-64). Shurts also teaches that trusted stored procedure's write sensitivity label is dominated by an object's access sensitivity label, the trusted stored procedure can write to that object during execution. A subject's sensitivity labels need not dominate the trusted stored procedure's read and write labels in order for the trusted stored procedure to execute. In fact, a trusted stored procedure may access objects beyond the reach of the subject in normal operation (see column 3, lines 45-53). Therefore, at the time the invention was made it would have been obvious to modify the system of Edwards in such a way that the enforcement of sensitivity label dominance and the restriction of data transfer between subjects and objects associated with inconsistent sensitivity labels is combined to provide discrete access between objects beyond the reach of the subject in normal operation as taught in Shurts. One of ordinary skill in the art would have been motivated to combine the enforcement of sensitivity

label dominance and the restriction of data transfer to provide discrete access between objects beyond the reach of the subject in normal operation as taught by Shurts for allowing the subject to use the trusted stored procedure or a trigger to access certain objects having higher sensitivity levels than his or her own (see Shurts, abstract).

6. Referring to claim 2, Edwards teaches labeling with sensitivity labels all objects including network connections, file systems objects etc. (see column 5, lines 1-5).

7. Referring to claim 3, it is notoriously well known in the art to use a tag value and a label definition. One of ordinary skill in the art would have been motivated to use the tag values and the label definitions for comparing the labels.

8. Referring to claims 3, 4 and 12, Edwards teaches defining the hierarchical classification of the operating system (see Fig. 3 and 4).

9. Referring to claim 8, Edwards shows defining arbitrary relationships between sensitivity labels for the subjects and objects and mapping the arbitrary relationships (see Fig. 3).

10. Referring to claim 14, Edwards teaches mapping according to MAC (see column 3, lines 60-64).

11. Referring to claim 16, Edwards explicitly teaches mapping the controls with privileges such as read, write and execute (see column 5, lines 5-10).

12. With respect to the limitations of claims 17 and 22, the list of valid labels recited in the claims 17 and 22 is a standard list of Mandatory Access Control (MAC) protocol.

13. Regarding claim 18, it is well known in the art to separate labels by token "== >" and "P==>". One of ordinary skill in the art would have been motivated to use these tokens with ASCII code characters for easy recognition of the label.

14. Referring to claims 6 and 7, Edwards teaches interfacing with compartment mapping information on a real time basis.

15. Referring to the independent claim 24, the limitation " defining a fixed set of classifications for each subject and object .. " is met by the sensitivity labels, which are prioritized in such a way that it determines how objects having one sensitivity label can interact with the objects having different sensitivity label (see Edwards, Fig. 3). The limitation " defining a set of compartments for each label.." is met by is met by Fig. 2 showing separate system components involved in data transfer based on classification levels assigned by means of labels. The limitation " partitioning application process entities and network interface entities into unique compartments" is met by compartments that hold application processes entities" is met by teachings of Edwards stating that sensitivity labels are prioritized for MAC in a way that determines how processes or objects having one sensitivity label can interact with processes or objects having different sensitivity labels. The MAC separated compartments are met by the web browser and the application running on a user machine and a web server (see Figs. 2 and 4).

16. Referring to claim 27, the limitation " ... complete information separation between Virtual Vault components, network interfaces, each application content and every

deployed application component..." is met by Fig. 2 showing separate system components involved in data transfer based on classification levels assigned by means of labels.

17. Referring to claims 9 and 28, the limitation" providing Mandatory Access Control separation between the compartments that hold network interface entities and the compartments that hold application processes entities" is met by teachings of Edwards stating that sensitivity labels are prioritized for MAC in a way that determines how processes or objects having one sensitivity label can interact with processes or objects having different sensitivity labels. The MAC separated compartments are met by the web browser and the application running on a user machine and a web server (see Figs. 2 and 4).

Conclusion

18. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

U.S Patent No. 5,903,732

U.S Patent No. 5,845,068

U.S. patent No. 6,292,900 B1

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Grigory Gurshman whose telephone number is (571)272-3803. The examiner can normally be reached on 9 AM-5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571)272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Grigory Gurshman
Examiner
Art Unit 2132

GG

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100